

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

|                                |   |                      |
|--------------------------------|---|----------------------|
| SRI INTERNATIONAL, INC.,       | ) |                      |
|                                | ) |                      |
| Plaintiff,                     | ) |                      |
|                                | ) |                      |
| v.                             | ) | Civ. No. 04-1199-SLR |
|                                | ) |                      |
| INTERNET SECURITY SYSTEMS,     | ) |                      |
| INC. (a Delaware corporation), | ) |                      |
| INTERNET SECURITY SYSTEMS,     | ) |                      |
| INC. (a Georgia corporation)   | ) |                      |
| and SYMANTEC CORPORATION,      | ) |                      |
|                                | ) |                      |
| Defendants.                    | ) |                      |

**MEMORANDUM ORDER**

At Wilmington this 17<sup>th</sup> day of October, 2006, having heard oral argument and having reviewed the papers submitted in connection with the parties' proposed claim construction;

IT IS ORDERED that the disputed claim language in United States Patent Nos. 6,484,203 ("the '203 patent"), 6,708,212 ("the '212 patent"), 6,321,338 ("the '338 patent") and 6,711,615 ("the '615 patent"), as identified by the above referenced parties, shall be construed consistent with the tenets of claim construction set forth by the United States Court of Appeals for the Federal Circuit in Phillips v. AWH Corp., 415 F.3d 1303 (Fed. Cir. 2005), as follows:

1. **Terms of art applicable to all patents in suit:**

a. **"Network"**: A collection of software and/or hardware interconnected by communication links for sharing information.

b. **"Packet"**: A group of data bytes which represents a specific information unit with a known beginning and end.

c. **"Event"**: An action or occurrence detected by software.

2. **"Network monitors"**:<sup>1</sup> Software and/or hardware that can collect, analyze and/or respond to data.

The above limitation has been construed broadly, as the words used are words well known in the art and it does not appear from the specification<sup>2</sup> that the patentees were acting as their own lexicographers. The court recognizes, consistent with defendants' proposed construction, that the specification does describe the network monitors as using "the same monitor code-base" to provide a "reusable software architecture" that accommodates "[c]ustomizing and dynamically configuring" the monitors. ('203 patent, col. 10, ll. 29-36) However, the disputed claim language does not track the language of the specification and the court declines to read further limitations

---

<sup>1</sup>All patents, multiple claims.

<sup>2</sup>Because this limitation is included in all the patents in suit and in multiple claims, and because the specifications of all the patents in suit are substantially similar, the court will refer to the specification of the '203 patent unless otherwise indicated.

into the claims.

3. **"Deploying a plurality of network monitors":**<sup>3</sup>

Configuring and/or installing two or more network monitors.

Consistent with the above construction of "network monitor," software is configured and hardware is installed.

4. **"Hierarchical event monitoring [and analysis]":**<sup>4</sup>

Network monitors, arranged in two or more levels, interoperate in order to analyze and respond to network activity.

('203 patent, col. 2, ll. 56-65; col. 9, ll. 21-34)

5. **"Hierarchical monitor/hierarchically higher network monitor":**<sup>5</sup> A network monitor that receives data from at least one network monitor that is at a lower level in the analysis hierarchy.

('203 patent, col. 2, ll. 56-65; col. 3, ll. 51-55)

6. **"Service monitor":**<sup>6</sup> A network monitor that provides local real-time analysis of network packets transmitted by a network entity, such as a gateway, router, firewall or proxy server.

('203 patent, col. 2, ll. 66 to col. 3, ll. 2)

---

<sup>3</sup>'203, '212 and '615 patents, multiple claims.

<sup>4</sup>'203 and '615 patents, multiple claims.

<sup>5</sup>'203, '212 and '615 patents, multiple claims, and '338 patent, claim 13.

<sup>6</sup>'203, '212 and '615 patents, multiple claims.

7. **"Domain monitor":**<sup>7</sup> A network monitor that receives and analyzes data from service monitors.

('203 patent, col. 3, ll. 23-27)

8. **"Enterprise monitor":**<sup>8</sup> A network monitor that receives and analyzes data from domain monitors.

('203 patent, col. 3, ll. 43-44)

9. **"Peer-to-peer relationship":**<sup>9</sup> A relationship between two or more network monitors at the same level in an analysis hierarchy which allows the monitors to share data.

('203 patent, col. 3, ll. 32-36)

10. **"Automatically receiving and integrating reports of suspicious activity":**<sup>10</sup> Without user intervention, receiving reports of suspicious activity and combining those reports into a different end product; i.e., something more than simply collecting and reiterating data.

('203 patent, col. 7, ll. 37-54 and ll. 64 to col. 8, ll. 3; D.I. 266, ex. P)

11. **"Correlating/correlates":**<sup>11</sup> Combining the reports to

---

<sup>7</sup>'203, '212 and '615 patents, multiple claims.

<sup>8</sup>'203, '212 and '615 patents, multiple claims.

<sup>9</sup>'203, '212 and '615 patents, multiple claims.

<sup>10</sup>'203, '212 and '615 patents, multiple claims.

<sup>11</sup>'203, '212 and '615 patents, multiple claims, and '338 patent, claim 15.

reflect underlying commonalities.

('203 patent, claim 2 at col. 14, ll. 36-38)

12. **"Responding . . ./invoking countermeasures":**<sup>12</sup> Taking an action in response, including both passive and active responses.

('203 patent, col. 11, ll. 33-44)

13. **"Building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets":**<sup>13</sup> Generating at least two separate data structures, one a statistical description representative of historical network activity, and one a statistical description of recent network activity, where the statistical descriptions are based on at least one measure of the network packets and are generated through the use of statistical analysis; i.e., something more than simply collecting and retrieving data.

('338 patent, col. 5, ll. 36-52; col. 6, ll. 38-60; col. 12, ll. 47-52; D.I. 268, ex. N)

The specification incorporates by reference a specific statistical analysis technique disclosed in "A. Valdes and D. Anderson, 'Statistical Methods for Computer Usage Anomaly Detection Using NIDES', Proceedings of the Third International Workshop on Rough Sets and Soft Computing, January 1995." ('338

---

<sup>12</sup>All patents, multiple claims.

<sup>13</sup>'338 patent, multiple claims.

patent, col. 5, ll. 41-49) Although the court acknowledges that the specification also indicates that the "profile engine can use a wide range of multivariate statistical measures to profile network activity indicated by an event stream" ('338 patent, col. 5, ll. 37-39), nevertheless, the court concludes that the specification and referenced article require that some manipulation of the data take place; i.e., generating a "statistical" profile means more than collecting and retrieving data.

14. **"Determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity":**<sup>14</sup> Using the result of the comparison to decide whether the monitored activity is suspicious.

('338 patent, col. 12, ll. 47-65)

15. **"A statistical detection method":**<sup>15</sup> A method of detecting suspicious network activity by applying one or more statistical functions in the analysis of network traffic data. This method is not a signature matching detection method.

('212 patent, col. 5, ll. 46-61; claim 3 at col. 15, ll. 19-21)

---

<sup>14</sup>'338 patent, claims 1, 11, 21, 24 and 25)

<sup>15</sup>'212 and '615 patents, multiple claims.

16. **"A signature matching detection method":**<sup>16</sup> A method of detecting suspicious network activity by comparing observed network traffic data to known patterns.

('212 patent, col. 7, ll. 33-51)

17. **"A virtual private network":** A network that uses encryption to securely transmit network packets via a public network.

This is an agreed upon construction.

18. **"Firewall":** An interface between two networks that enforces a security policy.

This is an agreed upon construction.

19. **"Proxy server":**<sup>17</sup> A server that mediates communication between a client application, such as a Web browser, and a real server. It handles requests to the real server to see if it can fulfill the requests itself; if not, it forwards the requests to the real server. The proxy server can serve as a firewall component.

(D.I. 266, ex. M at SYM\_P\_0498228)

20. **"API":**<sup>18</sup> The interface between the application software and the application platform, across which all services are provided.

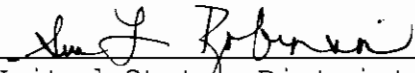
---

<sup>16</sup>'212 patent, multiple claims.

<sup>17</sup>All patents, multiple claims.

<sup>18</sup>'203, '212 and '615 patents, multiple claims.

(D.I. 266, exs. R, S)

  
United States District Judge